quadratorum imparium vor $8m+3$ in quocunque casu ipsius m angegeben werden könne, noch sehr dunkel. Es ist mir eingefallen, dass wenn man die drey radices quaesitas setzen möchte A, B, C, und

$$A = 1 + am + bmm + cm^3 + dm^4 + \text{etc.}$$
$$B = 1 + am - bmm - cm^3 - dm^4 - \text{etc.}$$

folglich

$$\begin{aligned} AA = 1 + 2am &+ 2bmm + 2cm^3 + 2dm^4 + 2em^5 + \text{etc.} \\ &+ aa \quad\;\; + 2ab \;\;\; + 2ac \;\;\; + 2ad \\ &\qquad\qquad\qquad\quad + bb \;\;\;\; + 2bc \end{aligned}$$

$$\begin{aligned} BB = 1 + 2am &- 2bmm - 2cm^3 - 2dm^4 - 2em^5 + \text{etc.} \\ &+ aa \quad\;\; - 2ab \;\;\; - 2ac \;\;\; - 2ad \\ &\qquad\qquad\qquad\quad + bb \;\;\;\; + 2bc \end{aligned}$$

und

$$\begin{aligned} CC = 1 &+ 8m - 2aamm \quad * \quad - 2bbm^4 - 4bcm^5 \\ &- 4a \end{aligned}$$

alsdann $AA + BB + CC = 8m + 3$ und alle coëfficientes b, c, d, etc. per solam a determinirt werden könnten, so dass a eine quantitas indeterminata bliebe, denn es wird posita

$$C = 1 + \alpha m + \beta mm + \gamma m^3 + \delta m^4 + \text{etc.}$$
$$\alpha = 4 - 2a,\quad \beta = -2aa - \alpha\alpha,\quad \gamma = -2\alpha\beta, \text{etc.}$$

hieraus würde ferner folgen, dass wenn das theorema an sich selbst wahr ist, die series A, B, C allezeit numeris integris gleich seyn würden, man möchte auch vor a annehmen, was man wollte.

Goldbach.

LETTRE CXIII.

=

Euler à Goldbach.

Sommaire. Suite des recherches précédentes. Théorème de géométrie.

Berlin d. 23. Februar 1748.

Das über meinen vorigen Brief gehabte dubium wird sogleich wegfallen, wenn Ew. sich zu erinnern belieben werden, dass daselbst von numeris integris die Rede sey, denn da $P = 4pp - 1$, so kann in ganzen Zahlen P unmöglich ein Quadrat seyn; in Brüchen aber wäre solches auf unendliche Arten möglich.

Dass alle in dieser Formul $8m + 3$ enthaltenen Zahlen in drey quadrata imparia resolvirt werden können, bin ich noch keineswegs im Stand zu beweisen, ungeacht ich mir darüber den Kopf schon ziemlich verbrochen habe. So oft $8m + 3$ ein numerus primus ist, so ist dieselbe allzeit in dieser Form $2aa + bb$ enthalten, als $3 = 2.1 + 1$;

$11 = 2.1 + 9$; $19 = 2.9 + 1$; $43 = 2.9 + 25$, etc. und hievon getrauete ich mir noch die Demonstration zu finden. Ich glaube auch nicht, dass man für diese Proposition, dass $8m + 3 = aa + bb + cc$ eine solche Demonstration finden könne, wodurch die drey radices a, b, c selbst bestimmt werden, sondern man wird nur die possibilitatem resolutionis anzuzeigen im Stande seyn. Aus diesem Grunde habe ich zu dem von Ew. eingeschlagenen Weg kein grosses Vertrauen, weilen dadurch nicht nur die Möglichkeit gezeigt, sondern auch die tria quadrata selbst in genere angegeben werden könnten, welches letztere ich gleichwohl für unmöglich halte. Die Demonstration müsste ungefähr meines Erachtens derjenigen ähnlich seyn, wodurch ich bewiesen, dass omnis numerus primus $4n + 1$ eine summa duorum quadratorum sey. Ich beweise erstlich, dass eine jede summa duorum quadratorum $aa + bb$ (wo a et b numeri inter se primi gesetzt werden) keine andere divisores haben könne, als welche gleichfalls summae duorum quadratorum sind. Hernach so oft $4n + 1$ ein numerus primus ist, kann ich unendlich viel Zahlen hujus formae $p^{2n} + q^{2n}$ angeben, welche durch $4n + 1$ divisibel sind. Da nun $p^{2n} + q^{2n}$ eine summa duorum quadratorum ist, so muss auch $4n + 1$ als ein divisor derselben Formul gleichfalls eine summa duor. quadr. seyn. Die resolutio autem ipsa in duo quadrata wird hierdurch nicht offenbar, sondern nur die Möglichkeit derselben bewiesen.

Man kann aber diese Proposition, dass $8m + 3$ allzeit eine summa trium quadratorum sey, in vielerley andere Formen einkleiden, welche vielleicht leichter zu demonstriren seyn dürften. Als, wenn man beweisen könnte, dass proposito numero quocunque integro m, für p und q allzeit

solche Werthe anzugeben möglich wären, so dass nachfolgende aequatio cubica

$$x^3 - (2p - 1)xx + (2pp - 2p - 1 - 4m)x - q = 0$$

alle drey radices rationales überkäme, so wäre die Sach auch bewiesen. Denn wenn a, b, c die radices dieser Aequation wären, so würde $2p - 1 = a + b + c$, et

$$2pp - 2p - 1 - 4m = ab + ac + bc.$$

Weil nun

$$4pp - 4p + 1 = aa + bb + cc + 2ab + 2ac + 2bc,$$

so subtrahire man davon

$$4pp - 4p - 2 - 8m = 2ab + 2ac + 2bc$$

so bleibt übrig $8m + 3 = aa + bb + cc$. Ich habe aber hiezu schlechte Hoffnung, weil die Demonstration nur auf valores integros ipsius m gehen müsste; denn in fractis wäre die Sach oft unmöglich.

Ich habe diese Sach auch folgendergestalt betrachtet: Es muss allzeit möglich seyn von $8m + 3$ ein solches Quadrat $4xx - 4x + 1$ zu subtrahiren, dass der Rest

$$8m + 2 - 4xx + 4x$$

in zwey quadrata resolubel werde. Folglich muss auch die Hälfte davon $4m + 1 - 2xx + 2x$ eine summa duor. quadr. seyn, nehmlich $4yy - 4y + 1 + 4zz$, also würde

$$m = \frac{xx - x}{2} + yy - y + zz.$$

Wenn man dahero beweisen könnte, dass diese Formul $\frac{xx - x}{2} + yy - y + zz$ alle numeros integros in sich begreife, so wäre das theorema auch bewiesen.

Fermat sagt in seinen Observationibus ad Diophantum, dass diese Aequation $x^n = y^n + z^n$ in numeris rationalibus allzeit unmöglich sey, exceptis casibus $n = 1$ et $n = 2$, nehmlich weder eine summa duorum cuborum könne ein cubus, noch eine summa duorum biquadratorum ein biquadratum, noch in genere eine summa duarum potestatum altiorum eine gleiche potestas seyn. Er sagt, dass er dafür eine sehr ingenieuse Demonstration habe, welche er aber wegen Mangel des Raums nicht beysetzen könne. Es ist also sehr schad, dass auch diese nebst vielen andern verloren gegangen.

Ich bin neulich auf nachfolgendes theorema geometricum gefallen, welches mir merkwürdig zu seyn scheinet. Nehmlich, gleich wie in einem jeden parallelogrammo die summa quadratorum laterum der summae quadratorum diagonalium gleich ist, so ist in einem jeden quadrilatero non parallelogrammo die summa quadratorum laterum grösser als die summa quadratorum diagonalium, und der excessus kann also concinne angegeben werden: Man bisecire (Fig. 28) in dem trapezio $ABCD$ die diagonales AC und BD in N et M und jungire die Linie MN, so wird seyn:

$$AB^2 + BC^2 + CD^2 + DA^2 = AC^2 + BD^2 + 4MN^2.$$

Euler.

LETTRE CXIV.

=

Goldbach à Euler.

Sommaire Suite des recherches arithmétiques.

St Petersburg d. 6. April 1748.

In Ew. Schreiben vom 2. Sept. hatte ich die Worte: *dass P um 1 immer kleiner als ein Quadrat seyn muss*, für eine zur vorhergehenden Formul $Q = P + \sqrt{(2PP \pm 2)}$ gehörige Condition angesehen, welche sich aber, wie ich nunmehro finde, blos auf die Aequation $zz = 4pp - 1 = P$ rapportiren, so dass alles seine Richtigkeit hat.

Wenn Ew., wie Sie vermuthen, demonstriren könnten, dass alle numeri $8m + 3$, wenn sie primi sind, zu dieser Formul $2aa + bb$ gebracht werden können, so werden Sie auch leicht finden, dass alle numeri primi $4m + 3$ zu dieser Formul gehören $2aa + bb + cc$, weil dieselbe meines Erachtens alle numeros impares in sich begreift; wenn aber